

# A New Approach For Mobile

8 elements of a complete mobile app environment By Michael Finneran

Mobile application development is a new animal, and IT leaders shouldn't expect to tame it using their same old tricks. Driven by the growing number of smartphones and tablets, along with higher capacity mobile networks, companies are looking at how they can use mobile tools to transform their core processes and business models. To get those results, IT must create an application life-cycle management approach that specifically addresses the unique problems mobility creates.

IT needs mobile application life-cycle management that addresses development, distribution, security, support, and enhancement. These are areas IT must plan out before starting the development process because they'll impact the app development approach organizations take.

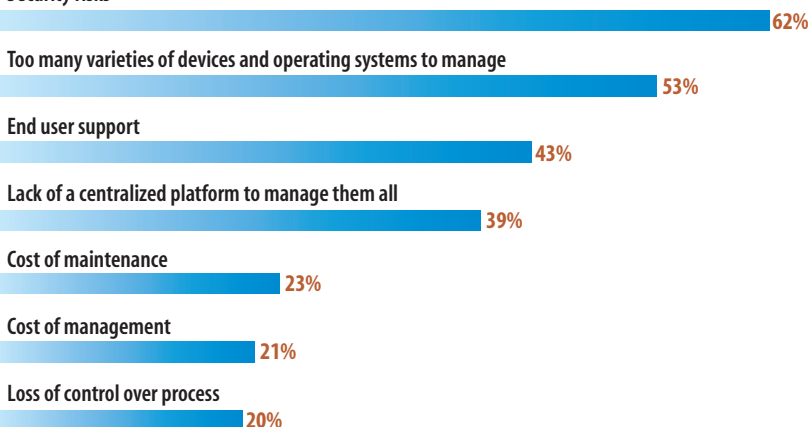
And IT teams must deliver these new mobile capabilities in a rapidly changing environment. While mobile operators are rolling out higher speed services, they're also cutting back unlimited data plans. Many businesses are shifting away from devices the company buys to ones that employees own. This BYOD (bring your own device) approach means that IT has to support more platforms, providing security and management in this new, free-wheeling environment.

The main challenge will be supporting enterprise applications on Apple iOS, Android, Windows Mobile, and

## Device And OS Worries

What are your top concerns over the growing number of devices and operating systems that you may need to support?

### Security risks



Data: InformationWeek Analytics OS Wars Survey of 343 business tech pros concerned about supporting a growing number of devices and operating systems, May 2011

other operating systems, in an environment where the user, not IT, decides when to upgrade the OS.

A recent *InformationWeek Analytics* survey of 441 business technology professionals found that 78% are either "somewhat" or "very" concerned about supporting the growing number of devices and operating systems. Security led the list of concerns, cited by 62% of respondents, followed by too many devices and operating systems to manage (53%), end user support (43%), and a lack of a centralized platform to manage them all (39%). These concerns are well founded, given that few respondents have antivirus software and patch management and software deployment tools on smartphones (13% for each).

The first step in addressing a mobile application development strategy is to understand the scale and the nature of the task. Mobility throws several new wrenches into the app dev process:

>> Mobile devices are easily lost or stolen, increasing security risks.

>> Mobile networks are slower and less reliable than regular networks, and they aren't always available.

>> Mobile data services are becoming more expensive, particularly with the demise of unlimited data plans. And if employees roam internationally, the costs can go through the roof.

>> Mobile devices have slower processors and less memory; battery life can be a limiting factor as well.

There are a number of design op-

tions available for mobile application projects. The approach you take will affect capital and operating expenses, functionality, and user experience. Before starting, think through the entire life cycle and make plans for each of these eight major elements.

### 1. The Development Environment

You can customize mobile apps for the screen size and user interface characteristics of the mobile devices you deploy or support. But that may not be the best choice if it means different versions of the app will be needed for each mobile ecosystem (BlackBerry, Apple iOS, Android, Symbian, Windows Mobile, Windows Phone 7, WebOS, etc.). Android alone has seven distinct releases in circulation.

Mobile enterprise application platforms, or MEAPs, can ease the development challenge by letting you develop one app that works across multiple platforms. The alternative is to develop a Web-based app and use the mobile browser. Tablets have introduced the potential for virtual desktop integration, using tools from vendors like Citrix and VMware; both have mobile clients.

### 2. Software Distribution

Once you have the application, the two main options for getting it to users are over-the-air distribution, where the app is sent to the device using a wireless data service, or syncing with a PC. While slower and potentially more costly, over the air is preferred because it's easiest for end users.

Alternatively, you can distribute apps through Apple's App Store, but companies must join Apple's iOS Developer Enterprise Program, and the app must be signed with a distribution certificate. Android apps must also be signed, and the posting party must register as an Android developer.

Companies that want to control their own software distribution can set up internal app stores using tools like EASE

from Apperian, or the app management capabilities found in mobile device management (MDM) systems like those from Airwatch, MobileIron, Sybase (now part of SAP), and Zenprise.

### 3. Maintenance, Patches, Upgrades

You also have to plan for distributing patches and upgrades. Mobile device management systems can help with this, too. Some systems provide automatic user notifications when an updated version of an app is available. At a minimum, administrators can blacklist the

to company data is to bar storing it on mobile devices. RIM's PlayBook tablet accesses corporate email, calendar, and contacts through the BlackBerry smartphone using a Bluetooth interface called BlackBerry Bridge. If the Bridge connection is broken, all data is erased from the PlayBook.

Web-based applications are another a good way to keep data from falling into the wrong hands, but access to these apps must be tightly controlled. Web apps with SSL connectivity will encrypt the data in transit, even if the user is connected through a public hotspot. Applications without SSL should connect through a VPN, particularly if hotspot access is supported. The downside of this approach is that users can only access the app if they have serviceable network connectivity.

SSL-based access provides over-the-air security, but users can still cut-and-paste on mobile devices to copy sensitive data from Web applications and into documents on the device.

If sensitive information is going to reside on the device, security issues start to multiply. At a minimum, you must ensure that data on the device is encrypted, a strong password is required to power it on, and all information on the device can be wiped remotely. You also must be able to wipe all company information if the user leaves, even if it's a user-owned device.

Policy enforcement and remote wipe are standard capabilities on MDM systems, but other requirements can be more difficult. Not all mobile operating systems support onboard encryption. For example, Android 2.2, the most widely deployed version of the OS, doesn't support on-device encryption. Android 3.0 does, but only on tablets. The Android 4.0 release, called Ice Cream Sandwich, will run on both smartphones and tablets and will likely include on-board encryption. It's due next year.

Finally, if users will be moving in

---

## 6 Steps To A Mobile App Business Plan

---

1. Start slow, but get started!
  2. Identify potential apps to pursue
  3. Determine the range of platforms to support and define the application—its functions, performance requirements, data volumes, etc.
  4. Identify management and support requirements
  5. Develop, pilot, evaluate, and refine
  6. Deploy it
- 

earlier version of an app and force users to upgrade. One problem with this approach is you don't want users who are traveling overseas where mobile charges are exorbitant to have to do an upgrade to access information they need.

You can do software distribution and maintenance without an MDM system, but it can be cumbersome, particularly if each user must download the app to a PC or laptop and then upload it to a smartphone. You end up paying a lot of help desk overtime every time you push out an upgrade, and you'll still need a way to ensure that all users installed it.

### 4. Security

Security is a top concern with mobile systems. One way to lower the risk

and out of wireless coverage, tools such as NetMotion Wireless's Mobility XE can maintain a persistent, secure (FIPS 140-2 compliant) VPN connection. That way, users don't need to log in and restart their applications every time they re-enter the coverage area.

The big problem with that approach is it's limited to Windows environments now, but NetMotion says it plans to address other mobile operating system environments as well.

### **5. User Support**

Some companies justify moving to user-owned devices as a way to save on support costs. But having employees solve their own IT problems isn't a good use of their time. The quirky nature of mobile connections and the relative newness of mobile technologies will lead to more, rather than fewer, support calls. Make sure you consider help desk training in your calculations.

### **6. Expense Management**

With the operators phasing out unlimited data plans, the cost of mobile network usage could rise. One way around that is to configure devices so that they first go to available Wi-Fi networks. Of course, if that includes

public hotspots, you must ensure there's a VPN or other encryption mechanism in place since public access points don't use any Wi-Fi encryption mechanisms.

Wireless expense management systems, such as those offered by Asentinel, Rivermine, and Tangoe, let you import the carrier's billing information, plot trends, highlight exceptions, and determine the most effective plan for each user. At a minimum, in your pilot test attempt to get a baseline of the amount of data traffic the mobile application creates so you can budget for the expense.

### **7. Support For New Platforms**

The deluge of new mobile devices won't abate anytime soon, so define how you'll test and certify your app on new devices. Two years ago, tablets weren't a blip on the horizon, and now they're everywhere. And don't think strictly in terms of new tablets and smartphones; imagine other purpose-built and specialized mobile appliances that will find their way into your network.

### **8. Your Mobility Policy**

Once you've plotted the overall strategy, incorporate it into your mobility policy. Spell out the range of devices

and operating system environments you'll support, the personal and business applications allowed, acceptable use, user responsibilities, and penalties for noncompliance, and all other management issues that govern mobility.

If you don't have a mobility policy, draft one. The Enterprise Mobility Forum, a think tank backed by several wireless vendors, provides an excellent template to help you to understand what to include. You can find it here: [informationweek.com/1307/emf](http://informationweek.com/1307/emf).

IT departments face huge challenges in planning mobile app development and deployment. Don't just think about "the app" but consider the entire management, security, and support complex that surrounds it in order to deliver a full-featured user experience. The learning curve may be steep, and there will be bumps along the way, but thinking through the whole process will let you deliver the business impact and ROI that will put you in good stead both with users and fellow business leaders.

*Michael Finneran is a consultant and industry analyst specializing in wireless technologies, mobile unified communications, and fixed-mobile convergence. Write to us at [iwletters@techweb.com](mailto:iwletters@techweb.com).*